УДК 004.056.55+347.440.14+004.738.5

Лісовий І.В.
Войтович О.П.
Волинець О.Ю.

РЕКОМЕНДАЦІЇ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ БЕЗДРОТОВИХ З'ЄДНАНЬ ІНТЕРНЕТУ РЕЧЕЙ

Вінницький національний технічний університет

Анотація

Проведено аналіз методів забезпечення безпеки бездротових з'єднань в системах Інтернету речей (IoT). У роботі розглянуті три основні рівні забезпечення безпеки: рівень сприйняття, мережевий рівень та прикладний рівень. На кожному рівні визначено загрози та запропоновані рекомендації для їх запобігання. Розглянуто методи захисту бездротових мереж від моніторингу трафіку, неавторизованого доступу та атак типу "людина всередині" і "Відмова в обслуговуванні" (DoS). Запропоновано ряд заходів безпеки, включаючи зміну налаштувань за замовчуванням, встановлення захисту адміністративного доступу та використання надійних протоколів аутентифікації.

Ключові слова: *безпека, бездротові з'єднання, Інтернет речей, IoT, загрози, захист, безпека мережі, рівні захисту, моніторинг трафіку, аутентифікація, захист доступу, захист даних, оновлення ПЗ, безпечність мережі, захист інформації*

Abstract

The article analyzes the methods of ensuring the security of wireless connections in Internet of Things (IoT) systems. The paper considers three main levels of security: the perception level, the network level, and the application level. At each level, threats are identified and recommendations for their prevention are proposed. Methods of protecting wireless networks from traffic monitoring, unauthorized access, and man-in-the-middle and denial-of-service (DoS) attacks are considered. A number of security measures are proposed, including changing the default settings, installing administrative access protection, and using strong authentication protocols.

Keywords: *security, wireless connections, Internet of Things, IoT, threats, protection, network security, protection levels, traffic monitoring, authentication, access protection, data protection, software updates, network security, information protection*

Вступ

Розширення застосування бездротових мереж, особливо в контексті Інтернету речей (IoT), викликає необхідність уважного управління їх безпекою. Прийняттям фахівцями з кібербезпеки різних рівнів захисту, починаючи від сприйняття до прикладного рівня, визначено стратегії та рекомендації, спрямовані на запобігання можливих загроз. Враховуючи різні вектори атак, від моніторингу трафіку до атак типу "Відмова в обслуговуванні" (DoS), важливо розглядати різні методи захисту, включаючи зміну налаштувань за замовчуванням, встановлення стійких паролів, та оновлення програмного забезпечення. Ці заходи, хоча не гарантують повної безпеки, сприяють складнішій роботі зловмисників та знижують загрози для систем IoT [1].

Результати дослідження

На сьогоднішній день експерти з кібербезпеки визначають три основні рівні забезпечення безпеки Інтернету речей (IoT), які обумовлені його архітектурою: рівень сприйняття, мережевий рівень та прикладний рівень [2].

Рівень сприйняття має забезпечувати надійну ідентифікацію об'єктів та зчитування інформації з сенсорів.

Мережевий рівень повинен забезпечувати повсюдний доступ, передачу і зберігання інформації. У межах мережевого рівня виділяють ще два підрівні: підрівень доступу (мережі чи канали зв'язку, що надають доступ до мереж вищого рівня глобальності) і підрівень основного обміну (Інтернет).

На прикладному рівні важливо забезпечити обробку та аналіз прийнятої інформації для прийняття оптимальних управлінських рішень та контролю за управлінням, додатками і послугами.

Більшість IoT систем на підрівні доступу використовують бездротові мережі зв'язку: персональні мережі (WPAN), локальні мережі (WLAN). Забезпечити безпеку бездротової мережі ще складніше, ніж захистити дротову мережу. В діапазоні дії точки доступу бездротова мережа відкрита для всіх, хто володіє відповідними обліковими даними.

Існує кілька форм загроз безпеці в бездротових мережах. Основні з них це [3]:

Моніторинг трафіку. Відстеження пакетів даних в незахищеній бездротовій мережі, використовуючи відповідні програмні засоби за допомогою яких можна повністю розшифрувати вміст пакетів даних.

Неавторизований доступ. Здійснення моніторингу виконуваних в мережі програм та отримання доступу до бездротової мережі, знаходячись поза приміщенням, де вона функціонує. Навіть якщо в бездротовій мережі задіяні механізми захисту, істотною загрозою є під'єднання до підставної точки доступу (rogue access point).

Атака типу «людина всередині». Розміщення фіктивного пристрою між легальними користувачами і бездротовою мережею, який буде імітувати дійсний. В результаті чого можна отримати доступ до управління сеансами зв'язку користувача, отримати паролі, важливі дані і навіть доступ до корпоративних серверів.

Атака відмови в обслуговуванні (DoS) – це атака, призначена для вимкнення комп'ютера або мережі. Цей тип атаки робить сайт або мережу недоступними для користувачів. Серйозність DoS-атаки залежить від того, до яких наслідків може привести вихід з ладу бездротової мережі [4].

Іншим методом припинення роботи більшості бездротових мереж є використання сильного радіосигналу, що «глушить» всі інші.

Єдиної і повністю надійної системи захисту IoT систем, що застосовують бездротові мережі не існує. Однак, дотримання досить простих рекомендацій дозволить значно знизити ризики та ускладнити роботу зловмисника щодо зламу системи IoT чи несанкціонованого доступу до інформації.

Система безпеки бездротових мереж найбільш часто реалізується в точці доступу або в місці, де здійснюється бездротове підключення до мережі тому рекомендується здійснювати [5]:

– зміна всіх налаштувань за замовчуванням;

– налаштування захисту адміністративного доступу;

– налаштування надійних протоколів аутентифікації зі стійкими паролями;

– включення шифрування;

– своєчасне оновлення мікропрограм.

Також не існує універсального способу протидії DoS-атакам всіх типів. Однак серед найбільш дієвих видів захисту дотримання таких правил безпеки: – встановлення та оновлення брандмауерів;

– постійне оновлення антивірусних програмних засобів;

– встановлення останніх оновлень, за допомогою яких ліквідовують недоліки в системі безпеки операційної системи; – використання довгих паролів;

– від'єднання мережевих пристроїв, які не використовуються.

Як засоби додаткового захисту бездротових мереж можна рекомендувати: фільтрацію за MAC адресою; приховування SSID; заборону доступу до налаштувань точки доступу чи маршрутизатора через бездротову мережу [6].

Навіть незважаючи на застосування зазначених вище рекомендацій не можна гарантувати повної безпеки IoT системи. Тому, при виборі нових пристроїв з підтримкою бездротового зв'язку, що підключаються до всеосяжного Інтернету, слід особливу увагу звертати на появу нових функцій захисту бездротової мережі.

Висновки

Забезпечення безпеки в системах Інтернету речей (IoT) вимагає комплексного підходу на рівнях сприйняття, мережі та прикладництва. Загрози включають моніторинг трафіку, несанкціонований доступ та атаки DoS. Захист включає зміну налаштувань, використання надійних протоколів та додаткові заходи безпеки, такі як фільтрація MAC адреси. Гарантувати повну безпеку IoT складно, тому важливо уважно обирати пристрої та слідкувати за новими функціями захисту.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Гарник М. О. Все про IoT / М. О. Гарник. – Львів, 2021. – 38 с.

2. IoT: тільки факти? Основна ідея IoT все взаємопов'язане. Упорядкування речей [Електрон. ресурс]. – Режим доступу: https://silogic.group/ua/iot-top3-reasons-ua/

3. Lake, D., Rayes, A., and Morrow, M., "The Internet of Things," The Internet Protocol Journal, Volume 15, No. 3, September 2012.

4. Микитишин А.Г. DosAttack: DoS attacks: what is Denial of Service? // Independent Research Proje – ct. – 2020. – P. 1–24. URL: https://elartu.tntu.edu.ua/bitstream/123456789/16930/5/Mykytyshyn_A_G_Mytny – M_Kompjuterni_merezhi_Knyga_1.pdf

5. Buterin V. Open-Source IoT Platform [Електрон. ресурс] – Режим доступу: https://github.com/thingsboard

6. Important Things to Know About Wi-Fi Network Name (SSID) [Електрон. ресурс]. – https://nordvpn.com/ru/blog/chto-takoye-ssid/

Лісовий Іван Вадимович — студент групи 1БС-20б, Факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail ivanlisovy@gmail.com

Lisovij Ivan. V. — student 1BS-20b, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail ivanlisovy@gmail.com

Войтович Олеся Петрівна — к. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, e-mail voytovych.vk.vntu.edu.ua

Voytovych Olesya P. — Ph.D., Associate Professor of the Department of Information Protection, Vinnytsia National Technical University, Vinnytsia, e-mail voytovych.vk.vntu.edu.ua

Волинець Олександр Юрійович — асистент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, e-mail ovolynets@vntu.edu.ua

Volynets Oleksandr Y. — assistant at the Information Protection Department, Vinnytsia National Technical University, Vinnytsia, e-mail ovolynets@vntu.edu.ua